Date 11/01/2012

Environmental Management Consolidated Business Center (EMCBC)

Subject: Configuration Management of Computer Systems and Networks

Procedure

APPROVED: _ *Signature on File* ___
EMCBC Director
ISSUED BY: Office of Information Resource Management

1.0 PURPOSE

The purpose of this procedure is to define the methods and process to control the configuration of all components that define the cyber security boundary of the Environmental Management Consolidated Business Center (EMCBC) Information Technology (IT) systems.

2.0 SCOPE

All IT functions within the EMCBC and all Sites utilizing the EMCBC network systems or managed hardware.

3.0 APPLICABILITY

This procedure is applicable to all IT processes and systems managed by the EMCBC Office of Information Resource Management (IRM). This procedure is not applicable to systems connecting to the EMCBC "hotel type" internet provided for visitors.

4.0 REFERENCES

4.1 DOE O 200.1A, Information Technology Management

4.2 EMCBC PL-240-08 – Cyber Security–System Security Plan for General Support System:

4.2.1 AC-5 Separation of Duties
4.2.2 AC-6 Least Privilege
4.2.3 CM-1 Configuration Management Policy and Procedures
4.2.4 CM-2 Baseline Configuration
4.2.5 CM-3 Configuration Change Control
4.2.6 CM-4 Monitoring Configuration Changes
4.2.7 CM-5 Access Restrictions for Change
4.2.8 CM-6 Configuration Setting
4.2.9 CM-7 Least Functionality
4.2.10 MA-3 Maintenance Tools
4.2.11 RA-1 Risk Assessment Policy and Procedures
4.2.12 RA-3 Risk Assessment
4.2.13 SA-1 System and Services Acquisition Policy and Procedures

4.2.14 SA-3 Life-Cycle Support
4.2.15 SA-10 Developer Configuration Management
4.2.16 SA-11 Developer Security Testing
4.2.17 SC-1 System and Communications Protection Policy and Procedures
4.2.18 SC-14 Public Access Protections

5.0 DEFINITIONS

5.1 Cognizant Assistant Director: Assistant Director that is the controlling subject matter expert for a given application.

5.2 Configuration Control Board (CCB): Consists of the Assistant Director for the Office of Information Resource Management (ADIRM) (Chair), CCPM, and Member at Large. Reviews proposed changes and accepts, rejects, or places them on hold based on risk or significant impact to work processes.

5.3 Configuration Control Point Manager (CCPM): The IRM staff member(s) responsible for a particular Configuration Control Point (Desktop, Network, Applications, and Server).

5.4 Content Manager: Individual assigned by the Content Owner to manage the development of the application and to ensure the integrity of the data.

5.5 Content Owner: The EMCBC Assistant Director responsible for the content and functionality within the given application or system.

5.6 IRM Support Staff: IRM staff responsible for assisting in the completion of all required documentation related to the development and maintenance of applications, EMCBC network systems and managed hardware.

5.7 Member at Large: Member of the IRM staff who is not the CCPM who is appointed by the ADIRM for the purpose of serving on the Configuration Control Board.

5.8 System Owner: The lead IRM individual that has overall implementation responsibility for any given application. Usually the ADIRM.

5.9 Technical Documents: Internal Technical Documents controlled by IRM in accordance with written procedure.

5.10 Technical Owner / Developer: IRM staff responsible for coding, testing, and placing the application into production, and maintaining the application.

6.0 RESPONSIBILITIES

6.1 Assistant Director for the Office of Information Resource Management:

6.1.1 Chairs the Configuration Control Board;

6.1.2 Approves Configuration Baseline Changes;

6.1.3 Approves Configuration Checklists.

6.2 Configuration Control Point Manager:

6.2.1 Manage the Configuration of his/her assigned control point;

6.2.2 Develop Baseline Changes as appropriate;

6.2.3 Ensure that noted risks are updated in the Risk Portfolio Manager (RPM) database.

7.0 GENERAL INFORMATION

The configuration management plan is structured to address the different aspects of the many computer systems that make up the EMCBC IT infrastructure. IRM has many diverse elements, from Blackberry handhelds to servers handling multiple databases. This procedure provides for processes to establish baselines for each of the main configuration areas and then provides for controlled change and expansion of the system to meet the growing IT service area of the EMCBC. The plan provides for methods where security configurations are not defined by specific benchmarks, but where there is technical literature that will support development of secure configurations.

8.0 PROCEDURE

8.1 Initial Baselines – Initial Baselines are established at the time of Certification and Accreditation or may be subsequently established as new hardware, software or new applications are added to the system.

8.1.1 Development of Initial Baselines - Baselines are developed by the application of DOE standard configurations, as in the case of the DOE Common Operating Environment (DOECOE) for desktops, or the use of benchmarks such as the Center for Internet Security (CIS), and Defense Information Security Agency (DISA) standards for Servers, or if standards or benchmarks do not exist, IRM will develop a baseline configuration based on industry understanding of risks as outlined in trade literature (for example: disabling the use of “magic quotes” in PHP (a hypertext language). Such in-house baseline checklists will be documented in the form of a **Technical Document** and will be reviewed periodically to ensure that new risks are addressed and added to the Configuration Control Checklist.

8.2 Configuration Management - The EMCBC Configuration Management system is separated into four distinct Configuration Control Points (CCP): Desktops, Servers, Network Configuration, and Applications. Each Configuration Control Point will be assigned a Manager (CCPM). The CCPM is responsible for ensuring that his/her CCP meets the requirements of this procedure.

8.2.1 Desktop Configuration – The EMCBC uses the DOECOE Desktop image as the baseline configuration for all desktops. The DOECOE is updated as versions are issued by the Office of the Chief Information Officer (OCIO). In addition, the EMCBC may deploy additional software over and above the standard software suite provided by the DOECOE. These additions will be documented and approved by the ADIRM and documented as risks if appropriate in RPM.

8.2.1.1 Laptops – Laptop configurations are developed by manufacturing type. The CIS standards establish laptop configuration. Users may be allowed limited administrative rights on laptops to facilitate their use off site.

8.2.2 Server Configuration – The EMCBC uses CIS and DISA benchmarking tools to establish baselines for Server Configurations.

8.2.2.1 Each server will be benchmarked to the appropriate tools based on the function of the server. For example the web-server may have a different benchmark score than the server used to support the CBC-intranet.

8.2.2.2 Minimum scoring levels will be established by the ADIRM in accordance with guidance from DOE Headquarters or based on industry standards.

8.2.2.3 Additional Server Configurations are established based on Database Management Systems or web services that “sit” on top of the Server Operating System software. These include such software systems as PHP, Microsoft SQL (MSSQL), etc. This type of software is baselined by using the checklist and vulnerability scanning methods if benchmarks are not available.

8.2.3 Network Configuration – Network configuration is documented by a network diagram(s) showing the interconnections of the network and by documentation of the settings of the security equipment, such as firewalls, router, intrusion detections equipment, etc.

8.2.3.1 Network Diagrams are approved by the ADIRM and the settings on all network appliances are established and approved using the Baseline Configuration Change Form. Note that for clarifications the Voice Over Internet Protocol (VoIP) phones are considered to be a network item (because besides being a phone they are a switch) while the VoIP Server (Media Gateway Controllers) are controlled through server configuration control.

8.2.4 Application Configuration (EMCBC) – Applications Baselines are established by application of security checklists and vulnerability scans.

These types of checklists establish requirements for coding standards and address issues such as code injection attacks and information control.

8.2.4.1 IRM will maintain a list of the version of the software, the status, and the results of the latest configuration checklist. This requirement only applies to EMCBC developed or maintained applications.

8.3 Baseline Configuration Change – Baseline changes are developed and documented on a Baseline Configuration Change Form. Anyone working on a project or application may propose a change.

8.3.1 The proposed change is reviewed by the Configuration Control Board (CCB) made up of the ADIRM (Chair), the CCPM, and the Member at Large. Changes may be accepted, rejected, or put on holding pending the need for additional information or the need for off network testing.

8.3.2 The CCB will determine if the system or application needs to be re-baselined by application of the checklist or rerunning of a benchmark tool.

8.3.3 The CCB will also determine if there is any residual risk that requires documentation in RPM. The CCPM will be responsible for ensuring that the risks in RPM are updated.

8.3.4 The CCB will determine if the change will impact the Interconnect agreement with DOENet (and thus require completion of HQ CCP form).

8.3.5 The CCB will determine if the change will significantly impact any work process guided by a procedure or plan or other EMCBC document.

8.3.6 All members of the review board will sign the Baseline Configuration Change Form.

8.3.7 All changes made as a result of the CCB will be forwarded to the CCPM. The CCPM will ensure that once activated or installed all approved Baseline Configuration Changes are documented in the Information Management (IM) Maintenance Log.

8.3.8 Each CCPM shall ensure that the Least Functionality in accordance with PL-240-08, Cyber Security – System Security Plan for General Support System, is being maintained.

8.4 Minor Changes – Often during the course of system operations minor changes need to be made to options or settings of various hardware, software or applications to improve the functionality of the system or applications. These changes may be made by cognizant IRM staff to existing applications in the Configuration Baseline.

8.4.1 These types of changes are to be documented in the IM Maintenance Log. The log will be reviewed weekly by the Information System Security Officer (ISSO) to ensure that major changes that may affect the security posture have not been made without proper review.

8.4.2 A quarterly review by the Authorizing Official or designee will be conducted to determine if the aggregate effect of the minor changes requires base lining activity.

8.5 IM Maintenance Log - All actions such as changes, reviews, and audits, associated with the EMCBC Information Systems are documented in the IM Maintenance Log. Items that change configurations are indicated as such in the log.

9.0 RECORDS MAINTENANCE

9.1 Records generated as a result of implementing this document are identified as follows, and are maintained by the Office of Information Management and are managed in accordance with the EMCBC Organizational File Plan:

9.1.1 ADM 20-10.1-A - Software Development Case Files

9.1.2 GRS 24-08-C – Information Technology Operation and Management Records – IT Operations Records

10.0 FORMS USED – All Forms are the latest revision unless otherwise specified.

10.1 Configuration Change Proposal – Baseline Change Form, IMP-8308-02-F1

10.2 IM Maintenance Log - Sample

11.0 ATTACHMENTS

11.1 Attachment A - Configuration Change Proposal – Baseline Change Form, IMP-8308-02-F1

11.2 Attachment B - IM Maintenance Log - Sample

Attachment A

CM Information Resource Management EMCBC	**Configuration Change Proposal –Baseline Change**	Control Point:
	No.: BCP-20XX-000	Date:

Proposed Change

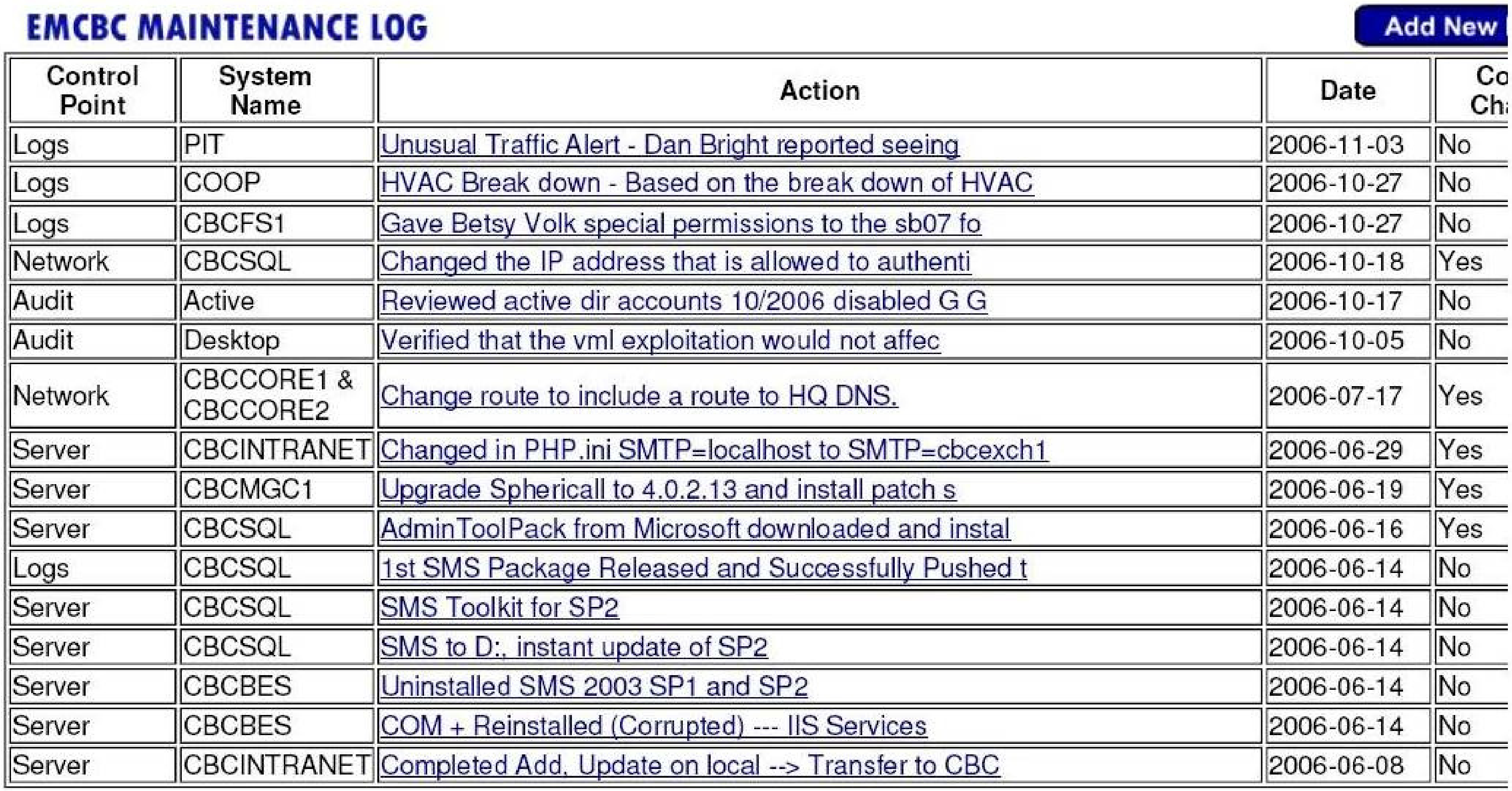
Additional Testing or Baseline Testing required?	**Yes** □	**No** □
Does this Change affect Interconnect with DOENet?	**Yes** □	**No** □
Does this Change significantly affect any documents, procedures, plans?	**Yes** □	**No** □

Impacted Systems and Applications:

APPROVED □ **REJECTED** □ **HOLD** □

Assistant Director for IRM:	Date:
Control Point Manager:	Date:
Member at Large::	Date:

Attachment B



EMCBC MAINTENANCE LOG

Control Point	System Name	Action	Date	Co Ch
Logs	PIT	Unusual Traffic Alert - Dan Bright reported seeing	2006-11-03	No
Logs	COOP	HVAC Break down - Based on the break down of HVAC	2006-10-27	No
Logs	CBCFS1	Gave Betsy Volk special permissions to the sb07 fo	2006-10-27	No
Network	CBCSQL	Changed the IP address that is allowed to authenti	2006-10-18	Yes
Audit	Active	Reviewed active dir accounts 10/2006 disabled G G	2006-10-17	No
Audit	Desktop	Verified that the vml exploitation would not affec	2006-10-05	No
Network	CBCCORE1 & CBCCORE2	Change route to include a route to HQ DNS.	2006-07-17	Yes
Server	CBCINTRANET	Changed in PHP.ini SMTP=localhost to SMTP=cbcexch1	2006-06-29	Yes
Server	CBCMGC1	Upgrade Sphericall to 4.0.2.13 and install patch s	2006-06-19	Yes
Server	CBCSQL	AdminToolPack from Microsoft downloaded and instal	2006-06-16	Yes
Logs	CBCSQL	1st SMS Package Released and Successfully Pushed t	2006-06-14	No
Server	CBCSQL	SMS Toolkit for SP2	2006-06-14	No
Server	CBCSQL	SMS to D:, instant update of SP2	2006-06-14	No
Server	CBCBES	Uninstalled SMS 2003 SP1 and SP2	2006-06-14	No
Server	CBCBES	COM + Reinstalled (Corrupted) --- IIS Services	2006-06-14	No
Server	CBCINTRANET	Completed Add. Update on local --> Transfer to CBC	2006-06-08	No

EMCBC RECORD OF REVISION

DOCUMENT - **Configuration Management of Computer Systems and Networks**

If there are changes to the controlled document, the revision number increases by one. Indicate changes by one of the following:

- Placing a vertical black line in the margin adjacent to sentence or paragraph that was revised.

- Placing the words GENERAL REVISION at the beginning of the text.

Rev. No.	Description of Changes	Revision on Pages	Date
0	Initial Information Management Procedure Supersedes IP-240-02, Rev. 2 dated 6/14/10	Entire Document	9/28/12